ARGUMENTS IN SUPPORT OF THE PRE-APPEAL REQUEST FOR REVIEW

Applicants respectfully submit that the rejections of record are based on clear factual deficiencies in the applied references. Accordingly, a *prima facie* case of obviousness under 35 U.S.C. § 103 is not established.

The Claimed Invention

The claimed invention relates generally to a system (independent claim 1) or method (independent claim 49) or computer-readable medium (independent claim 50) that provides protection from viruses.

These independent claims describe to various extents a firewall that classifies packets into those which can possibly contain a virus and those that cannot contain a virus. Those that are classified as of a type that cannot contain a virus are passed without further scanning. Those packets are of a type that can contain a virus are scanned to determine whether the packets indeed contain a virus. See Figure 1 and page 8, lines 9-17 of the specification. The specification provides an example of packets relating to audio and video data streams as types of packets that cannot contain viruses. See page 8, lines 17-20.

The Rejections of Record under 35 U.S.C. § 103

Pending claims 1 and 3-55 stand rejected over Fink (U.S. Patent No. 6,496,935) either alone or in combination with one or more of Franczek (U.S. Patent No. 6,397,335), Lyle (U.S. Patent No. 6,886,012), and Radatti (U.S. Patent No. 6,721,424).

Specifically, the claims stand rejected as follows:

- Claims 1, 3, 20-21, 32, 41-45, 47, 49-52, and 55 stand rejected under 35 U.S.C. § 103 over Fink ;
- Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 stand over Fink in view of Franczek ;
- Claims 6-8, 24-25, 34, and 54 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle;

- Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 stand rejected Fink in view of Lyle and Franczek; and
- Claim 40 stands rejected under 35 U.S.C. § 103 over Fink in view of Radatti.

These references, whether taken alone or in the combination asserted by the Examiner, fail to establish prima facie obviousness under 35 U.S.C. § 103.

A. THE PRIMARY REFERENCE FAILS TO TEACH OR SUGGEST THE CLAIMED FEATURE OF VIRUS SCANNING

The Examiner uses the primary reference Fink to reject claims 1, 49, and 50. Fink relates to a system for reducing computational work performed by firewalls. Fink filters packets to allow those packets from unknown sources to be scanned by a firewall. Packets from known trusted sources are permitted to enter a protected network without scanning. See Fink, column 2, lines 21-49. The sections relied upon by the Examiner relate to anti-spoofing systems controlled by Fink's prefiltering module 30. The prefiltering module checks packets to determine if they are related to a previously received packet. If the previously received packet was passed to the protected network 12, then the subsequently received related packets are passed to the protected network 12 without scanning by the firewall. See Fink, column 6, lines 24-33, and column 7, lines 33-47.

In contrast, each of the claims requires virus scanning. To address this deficiency of Fink, the Examiner on page 5 of the January 25, 2006, office action (lines 11-15) asserts that it would have been obvious to use virus scanning in Fink because

> "one would have been motivated to provide security by controlling the traffic being passed, thus preventing illegal communication attempts, both within single networks and between connected networks…"

The Examiner relies on column 7, lines 39-47, of Fink to show filtering at a firewall. However, the filtering of Fink relates to filtering packets to prevent the spoofing of packets. The Examiner seems to suggest that virus-infected packets can be eliminated by the prevention of spoofing.

This position lacks factual support. Whether or not a firewall receives a packet from a known source or an unknown source does not indicate whether the packet can contain a virus.

In response to Applicants' arguments of November 7, 2005, that Fink fails to teach or suggest virus scanning, the Examiner asserts

> "Fink discloses a virus (i.e. causing any kinds of violations and/or spoofing)…" (the January 26, 2006, Office Action, page 32, lines 11-13.)

Applicants strenuously object to the suggestion that Fink discloses any type of virus. There is no factual basis for believing that a spoofed packet includes a virus. Further, the code that performed the spoofing would have been resident at the entity sending the packet, not contained in the spoofed packet. There is no support for the Examiner's position that Fink discloses a virus.

Accordingly, because there is no teaching or suggestion to scan for viruses at all in Fink, no *prima facie* case of obviousness has been made. Thus, the rejections of claims 1, 49, and 50 must be withdrawn.

B. THE PRIMARY REFERENCE FAILS TO TEACH OR SUGGEST THE CLAIMED FEATURE OF CLASSIFYING PACKETS

The Examiner relies on Fink, column 6, lines 17-32, and column 7, lines 39-42, to suggest the claimed feature of the firewall classifying packets into

> "packets of a first type which cannot contain a virus and second type which can contain a virus…" (See claim 1.)

Fink fails to teach or suggest this recitation. Fink instead filters packets by determining if the packets have come from a trusted network as specified in the following section of Fink:

> "pre-filtering module 30 performs an anti-spoofing method. Since pre-filtering module 30 may optionally be connected to a plurality of networks, packets can come from any one of these networks. **The anti-spoofing method determines whether an IP packet, indicated as originating from a certain network, has indeed**

> **arrived from that network. As pre-filtering module 30 knows which network is connected to which interface, pre-filtering module 30 can determine whether a packet received from a particular interface is permitted**... Thus, if a packet comes from an allowed source node, is to be sent to an allowed destination, and has arrived through the expected interface, the packet can be processed by pre-filtering module 30." (Emphasis added) See column 7, lines 37-40, of Fink.

Fink fails to examine the type of the received packets and instead only examines the source of the packet. Stated differently, Fink differentiated between spoofed and non-spoofed packets. However, "non-spoofed" is not the same as "cannot contain a virus." For example, a packet containing a virus received from a known (but virus-infected) source would be passed to the protected network 12 by Fink's prefiltering module 30. Fink only pre-filters based on source/destination IDs and related information, and Fink assumes that a packet from a known ID must be safe. Fink is therefore vulnerable to viruses that have infected computers whose IDs must be recognized as "safe" by Fink's firewall.

As Fink fails to teach or suggest claim 1, no *prima facie* case of obviousness has been made. Claim 1 is allowable over Fink.

Independent claims 49 and 50 are similarly allowable over Fink.

C. THE SECONDARY REFERENCES

i. Franczek

The Examiner next applies Franczek (U.S. Patent No. 6,397,335) in combination with Fink (starting on page 13 of the office action). While Franczek teaches virus scanning, it does not teach allowing packets to pass through a firewall where the screening is based on the type of packets as required by the claims. This is the same failing from which Fink also suffers.

Rather, Franczek determines that whether the users are subscribed to the virus filtering system. See Franczek at Figure 3 (step 102) and column 5, lines 29-44. There is no teaching or suggestion in Franczek regarding the filtering of packets based on whether or not they can

contain a virus. In Franczek, all packets are either scanned or not scanned for viruses, irrespective of the extent to which they actually can contain a virus.

As there is no teaching regarding the filtering of packets as set forth in claim 1 and 50, no *prima facie* case of obviousness has been made. Claims 4-5, 11-14, 22-23, 27-28, 33, 36-37, 46, 48, and 53 are allowable over the combination of Fink in view of Franczek.

ii. Lyle

Claims 6-8, 24-25, 34, and 54 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle. As with Fink, Lyle fails to teach or suggest classifying received packets based on the type of packet. Like Fink, Lyle merely determines whether packets are from an authorized sender. As the combination fails to teach or suggest filtering based on packet type, no *prima facie* case of obviousness has been made. Claims 6-8, 24-25, 34, and 54 are allowable over the combination.

Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 stand rejected under 35 U.S.C. § 103 over Fink in view of Lyle and Franczek. As indicated above, none of Fink, Lyle, and Franczek teaches or suggests filtering based on whether a packet can contain a virus. Because there is no teaching in the applied references, no *prima facie* case of obviousness has been made. Claims 9-10, 15-19, 26, 29-31, 35, and 38-39 are allowable over the combination.

iii. Radatti

Claim 40 stands rejected under 35 U.S.C. § 103 over Fink in view of Radatti. Radatti fails to teach or suggest filtering packets based on whether or not they can contain viruses. In that Fink also fails to teach or suggest this feature of independent claim 1, no *prima facie* case of obviousness has been made. Dependent claim 40 is allowable over the combination.

CONCLUSION

For the above reasons, the rejections of pending claims 1, 3-51, and 53-55 in the Final Office Action fail to establish *prima facie* obviousness. A pre-appeal finding that these claims are allowable is respectfully requested.